

Reply to Comment on “Deterministic six states
protocol for quantum communication”
[arXiv:1107.4435v1 [quant-ph] / Phys. Lett. A
374 (2010) 1097]

October 7, 2011

J.S. Shaari^a, M. Lucamarini^b and Asma’ Ahmad Bahari^c

^{a,c}Faculty of Science, International Islamic University Malaysia (IIUM), Jalan
Sultan Ahmad Shah, Bandar Indera Mahkota, 25200 Kuantan, Pahang,
Malaysia

^bDipartimento di Fisica, Università di Camerino, Via Madonna delle Carceri, 9
62032, Camerino (MC), Italy

Abstract

We reply to the Comment made in arXiv:1107.4435v1 [quant-ph] (Phys. Lett. A **374** (2010) 1097) by noting some erroneous considerations therein resulting in a misleading view of the quantum key distribution protocol in question. We then correct the rates provided for the Intercept-and-Resend attack and we complete the analysis of Eve’s attack based on a double CNOT gate.

In the Comment reported in [1], the security analysis of the quantum key distribution protocol (QKD) introduced in [2] and named “6DP” was reviewed and partially criticized. The main point raised by the Comment is that in the analysis of selected attacks in [2], 6DP’s Control Mode uses two qubits from the same basis in contradiction with 6DP’s Encoding Mode where two qubits from different bases were selected for a reliable decoding process. The Comment proceeded with calculations and figures based on the notion that Alice chooses the same bases as that of Bob’s preparation for both the qubits in a pair in a control mode.

As we showed in [2] and will further clarify here, it is neither necessary nor efficient to follow such a prescription in the 6DP and analysis of half the qubit pair is sufficient.

In Ref. [1] two main attacks from the eavesdropper Eve are analyzed, the intercept-resend attack (IRA) and the double-CNOT attack (2CNOTA). In the

following, we report the security analysis for these two attacks thus demonstrating our claims. Moreover we correct a crucial feature of the 2CNOTA which was not captured in [1].

We begin with a brief description of 6DP; a two-way QKD protocol based on nonentangled qubits generalizing to the use of 3 mutually unbiased bases (MUB). In 6DP, two qubits are prepared by Bob in two different bases chosen randomly from 3 MUB and sent to and fro to Alice who will encode by executing 1 of 4 unitaries (3 Pauli spin matrices as well as the identity) on each qubit. Bob's sharp measurement of the received qubits would allow him to decode Alice's encoding. Security is achieved by having a control mode where randomly, Alice would with a certain probability make measurements in bases of her choice and through public discussions determine if an eavesdropper was in fact present.

Arguably the most straightforward eavesdropping strategy against 6DP is the IRA which foresees Eve making measurements of the traveling qubits in the bases of her choice on both the forward and backward path to glean a maximal amount of information of Alice's encoding.

The IRA was studied in [2] with the main purpose of showing that among all possible Eve's choices of measuring bases, the one including the same bases used by Bob, i.e. the canonical X , Y and Z , is the one which minimizes the detection probability. The analysis of Control Mode contained in [2] was limited to only one qubit at a time in the pair of qubits prepared by Bob. However this does not imply that Eve should necessarily attack one qubit only, nor does it imply that she should attack both qubits in the same basis (this was the allegation made in [1] regarding the analysis in [2]).

As we described above, the 6DP Encoding Mode is performed by using two different bases. It is then quite obvious that Eve should attack the protocol using two different bases, lest her information gain would not be maximized. In [2] we showed that the minimum probability for Eve to evade detection *per single qubit analyzed* by Alice and Bob is 0.5. Thus the legitimate parties could have inferred the presence of an eavesdropper in either half of the pair as long as their measurement basis coincides; which is certainly more probable than having both qubits measured in coinciding bases.

The Comment [1] further reported the probability to evade detection for Eve attacking twice in the same basis as 0.28, claimed for the sake of comparison to what the author had alleged of [2]. We stress that this had never been the case in [2] as such an attack has no relevance to the protocol where Eve would gain less information in doing so. To assume that Eve performs an attack which cannot provide her with maximal information is quite arguable and contrary to the principles usually followed in analyzing a quantum key distribution problem.

Finally, it is also suggested in Ref. [1] that Eve needs to measure the traveling qubits in the same basis as Bob's in order to gain from them the full amount of information encoded by Alice. This is hardly true. In fact, the measurements performed by Eve during the IRA effectively project the traveling qubits into

her measurement bases, which then are subjected to Alice's encoding. As noted in [2] (see Fig.1 and following discussion), Eve's best choice for the bases is any element of the set $\{XY, XZ, YZ, YX, ZX, ZY\}$, composed by all possible different bases combination, *irrespective of Bob's choice*. In this way, Eve is using exactly one of the same possible states as that of Bob, thus committing to a faithful decoding of Alice's unitaries and complete information thereof.

Let us now review the analysis of 2CNOTA reported in [1]. For that, it is useful to write the states prepared by Bob, $|0\rangle, |1\rangle, |x_+\rangle, |x_-\rangle, |y_+\rangle, |y_-\rangle$, as a single state $a|0\rangle + b|1\rangle$ with coefficients (a, b) given by $(1, 0), (0, 1), (1/\sqrt{2}, 1/\sqrt{2}), (1/\sqrt{2}, -1/\sqrt{2}), (1/\sqrt{2}, i/\sqrt{2})$ and $(1/\sqrt{2}, -i/\sqrt{2})$ respectively. The global evolution Bob's state and Eve's ancilla (those with subscript E) under the 2CNOTA is as follows:

$$\begin{aligned}\mathcal{I}_\pm^z (a|0\rangle + b|1\rangle) |0\rangle_E &\rightarrow (a|0\rangle - b|1\rangle) |0\rangle_E, \\ \mathcal{Y}_\pm^z (a|0\rangle + b|1\rangle) |0\rangle_E &\rightarrow (b|1\rangle - a|0\rangle) |1\rangle_E,\end{aligned}$$

where $\mathcal{I}_+^z \equiv \hat{C}(I \otimes I)\hat{C}$, $\mathcal{I}_-^z \equiv \hat{C}(Z \otimes I)\hat{C}$, $\mathcal{Y}_+^z \equiv \hat{C}(iY \otimes I)\hat{C}$ and $\mathcal{Y}_-^z \equiv \hat{C}(X \otimes I)\hat{C}$ and $\hat{C} \equiv CNOT$, with Eve's ancilla the target qubit and Bob's state the control qubit [3]. By a *single* execution of this attack Eve only can distinguish between the sets

$$S_{11} \equiv \{I, Z\}, S_{12} \equiv \{iY, X\},$$

but cannot distinguish between the two elements in each set. This means that by a single execution of the 2CNOTA, Eve cannot access the full 2-bit information encoded by Alice on each pair of qubits prepared by Bob. This fact was correctly noted in [1]. What was not noted is that by simply executing another 2CNOTA (on the other half of the qubit pair), Eve can easily access the full information. In fact, in the second 2CNOTA, Eve can use an ancilla in the state $|x_+\rangle_E$ rather than $|0\rangle_E$ and have her qubit in the position of the control and Bob's as the target [3].

With this choice, straightforward calculations (not presented here) reveals that the second 2CNOT allows Eve to distinguish between the sets

$$S_{21} \equiv \{I, X\}, S_{22} \equiv \{iY, Z\},$$

but not between the two elements in each set, in full analogy with what happens in the first 2CNOTA (it is just a change of basis). Hence, by comparing the results obtained in the two executions of the 2CNOTA, Eve can learn which operation was performed by Alice. For example, if Eve obtains S_{12} in the first 2CNOTA and S_{21} in the second 2CNOTA, then she will know that Alice encoded the operation X .

Quickly summarizing all of the above, security analysis in 6DP's Control Mode does not compel Eve to measure twice in the same basis while in the Encoding Mode, she is not obliged to measure in the same bases as Bob in order to steal full information from Alice through the IRA. Finally, although

a single execution of the 2CNOTA, as it was originally proposed in [2], cannot supply Eve with the full amount of information, a straightforward generalization including two executions of the 2CNOTA can, thus restituting importance to our original analysis about this attack. In conclusion, we have shown that the analysis contained in Ref. [1] contains a number of inaccuracies and in our present Reply we have corrected them, thus re-establishing the soundness of our original results.

Acknowledgement

One of the authors, J.S.S. would like to acknowledge financial support under the project FRGS0510-122 from the Ministry of Higher Education's FRGS grant scheme and the University's Research Management Centre for their assistance and facilities provided.

References

- [1] Faisal A. A. El-Orany, arXiv:1107.4435v1 [quant-ph], Phys. Lett. A 374 (2010) 1097.
- [2] J.S. Shaari, M. Lucamarini, M.R.B. Wahiddin, Phys. Lett. A 358 (2006) 85.
- [3] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2010).